

AMENDMENT TO THE CLAIMS

1-43 (canceled)

1 44. (currently amended): ~~The method of claim 38,~~ A method for providing a
2 capability to securely update information stored in a plurality of computer
3 systems, wherein the method comprises:

4 forming a protected partition within a hard drive of each of the computer
5 systems

6 storing, within nonvolatile storage of each computer system in the plurality
7 of computer systems, a setup password, an operating system, and an
8 initialization routine to execute within a processor of the computer system after
9 power on of the computer system, wherein the initialization routine includes
10 instructions causing the protected partition to be locked before the operating
11 system is loaded, wherein instructions causing information stored within the a
12 predetermined location to be written within the protected partition after
13 predetermined security procedures using the setup password have occurred but
14 before the protected partition is locked, and wherein the initialization routine
15 includes instructions causing the processor of the computer system to perform a
16 method including:

17 a) comparing information stored in the protected partition with
18 information from the update partition file stored within the predetermined
19 location;

20 b) when a portion of the information stored in the protected
21 partition is found to match a portion of the information stored within the
22 update partition file, overwriting the portion of the information stored in
23 the protected partition with the portion of the information stored in the
24 update partition file if space around the portion of the information stored
25 in the protected partition is sufficient;

26 c) when a portion of the information stored in the protected
27 partition is not found to match a portion of the information stored within
28 the update partition file, writing the portion of the information stored within
29 the update partition file to append to the information stored in the
30 protected partition if space within the protected partition is sufficient; and
31 d) locking the protected partition to prevent further modification
32 of information stored within the protected partition;
33 establishing a network connecting each computer system in the plurality of
34 computer systems with a server system;
35 generating an update partition file within the server system, wherein the
36 update partition file includes a plurality of entries and a plurality of encrypted
37 elements, wherein each entry within the plurality of entries includes information
38 to be stored at a different location within the protected partition, and wherein
39 each encrypted element within the plurality of encrypted elements is associated
40 with an entry in the plurality of entries,
41 transmitting the update partition file over the network to each computer
42 system in the plurality of computer systems;
43 ~~the method additionally comprises,~~ following determining that the update
44 partition file is stored within the computing system for updating the protected
45 partition, verifying whether each entry in the plurality of entries within the update
46 partition file has been generated by the server system, and
47 storing the update partition file within the predetermined location of each
48 computer system in the plurality of computer systems, wherein each entry in the
49 plurality of entries within the update partition file is written to the protected
50 partition only following verification that the entry has been generated by the
51 server system.

1 45. (previously presented): The method of claim 44, wherein verifying that
2 each entry in the plurality of entries within the update partition file has been
3 generated by the server system includes:

4 forming a first message digest by applying a hash algorithm to the entry;
5 forming a second message digest by signing the encrypted element
6 associated with the entry using a public key of the server system; and;
7 determining that the first and second message digests are identical.

1 46. (previously presented): The method of claim 44, wherein verifying that
2 each entry in the plurality of entries within the update partition file has been
3 generated by the server system includes signing the encrypted element
4 associated with the entry with a public key of the server system, and the
5 encrypted element of the update partition file has been prepared by signing,
6 with the private key of the server system, a result of the application of an
7 algorithm to data including a version of the setup password accessed by the
8 server system.

1 47. (previously presented): The method of claim 46, wherein
2 the data includes the version of the setup password appended to the
3 entry,
4 the algorithm is a hash algorithm generating a message digest, and
5 verifying that the entry has been generated by the server system includes
6 applying the hash algorithm to the setup password stored within the computing
7 system appended the entry to generate a first version of a message digest and
8 comparing the first version of the message digest with
9 a second version of the message digest obtained by signing the encrypted
10 element.

1 48. (previously presented): The method of claim 44, wherein
2 information stored in the protected partition is compared to each entry in
3 the plurality of entries within the update partition file,
4 when a portion of the information stored in the protected partition is found
5 to match the entry, the portion of the information stored in the protected partition
6 is overwritten with the entry if space around the portion of the information stored
7 in the protected partition is sufficient, and
8 when a portion of the information stored in the protected partition is not
9 found to match the entry, the entry is appended to the information stored in the
10 protected partition if space within the protected partition is sufficient.

1 49. (previously presented): The method of claim 48, wherein
2 the method additionally comprises receiving an input signal from a
3 keyboard of the computing system and comparing the input signal with a signal
4 corresponding to a setup password stored in non-volatile storage within the
5 computing system, and
6 the protected partition is left unlocked if the input signal matches the
7 signal corresponding to the setup password.

50-56. (canceled)

1 57. (currently amended): ~~The interconnected system of claim 51, wherein~~ An
2 interconnected system for providing updated information in a secure manner,
3 wherein
4 the interconnected system comprises a network, a server system
5 connected to the network and programmed to generate an update partition file
6 and to transmit the update partition file over the network; and a computer system
7 connected to the network,
8 the computer system includes a processor, non-volatile data storage
9 including a hard drive having a protected partition,

10 the processor is programmed to receive the update partition file from the
11 network and to store the update partition file in a predetermined location within
12 the nonvolatile data storage outside the protected partition.

13 the nonvolatile data storage stores an operating system and an
14 initialization routine, executing within the processor after power on of the
15 computer system, including instructions causing the protected partition to be
16 locked before the operating system is loaded, and instructions causing
17 information stored within the predetermined location to be written within the
18 protected partition after predetermined security procedures have occurred but
19 before the protected partition is locked.

20 the initialization routine includes instructions causing the processor of the
21 computer system to perform a method including:

22 comparing information stored in the protected partition with
23 information from the update partition file stored within the predetermined
24 location;

25 when a portion of the information stored in the protected
26 partition is found to match a portion of the information stored within the
27 update partition file, overwriting the portion of the information stored in
28 the protected partition with the portion of the information stored in the
29 protected partition if space around the portion of the information stored in
30 the protected partition is sufficient;

31 when a portion of the information stored in the protected partition is
32 not found to match a portion of the information stored within the update
33 partition file, writing the portion of the information stored within the update
34 partition file to append to the information stored in the protected partition
35 if space within the protected partition is sufficient; and

36 locking the protected partition to prevent further modification of
37 information stored within the protected partition;

38 the update partition file includes a plurality of entries and a plurality of
39 encrypted elements,

each entry within the plurality of entries includes information to be stored at a different location within the protected partition,

each encrypted element within the plurality of encrypted elements is associated with an entry in the plurality of entries.

the method additionally comprises, following determining that the update partition file is stored within the computing system for updating the protected partition, verifying whether each entry in the plurality of entries within the update partition file has been generated by the server system, and

each entry in the plurality of entries within the update partition file is written to the protected partition only following verification that the entry has been generated by the server system.

58. (previously presented): The interconnected system of claim 57, wherein verifying that each entry in the plurality of entries within the update partition file has been generated by the server system includes:

- forming a first message digest by applying a hash algorithm to the entry;
- forming a second message digest by signing the encrypted element associated with the entry using a public key of the server system; and;
- determining that the first and second message digests are identical.

59. (previously presented): The interconnected system of claim 57, wherein verifying that each entry in the plurality of entries within the update partition file has been generated by the server system includes signing the encrypted element associated with the entry with a public key of the server system, and the encrypted element of the update partition file has been prepared by signing, with the private key of the server system, a result of the application of an algorithm to data including a version of a setup password accessed by the server system.

1 60. (currently amended): The interconnected system of claim 59, wherein
2 the data includes the version of the setup password appended to a the
3 entry,
4 said algorithm is a hash algorithm generating a message digest, and
5 verifying that the entry has been generated by the server system includes
6 applying the hash algorithm to the setup password stored within the computing
7 system appended the entry to generate a first version of a message digest and
8 comparing the first version of the message digest with a second version of the
9 message digest obtained by signing the encrypted element.

1 61. (previously presented): The interconnected system of claim 57, wherein
2 information stored in the protected partition is compared to each entry in
3 the plurality of entries within the update partition file,
4 when a portion of the information stored in the protected partition is found
5 to match the entry, the portion of the information stored in the protected partition
6 is overwritten with the entry if space around the portion of the information stored
7 in the protected partition is sufficient, and
8 when a portion of the information stored in the protected partition is not
9 found to match the entry, the entry is appended to the information stored in the
10 protected partition if space within the protected partition is sufficient.

1 62. (previously presented): The interconnected system of claim 61, wherein
2 the method additionally comprises receiving an input signal from a
3 keyboard of the computing system and comparing the input signal with a signal
4 corresponding to a setup password stored in non-volatile storage within the
5 computing system, and
6 the protected partition is left unlocked if the input signal matches the
7 signal corresponding to the setup password.